REMARKS/ARGUMENTS

Reconsideration of this application is respectfully requested.

The rejection of claims 1-4 under 35 U.S.C. §102 as allegedly anticipated by Doherty '170 is respectfully traversed.

As clarified in the above amendment to claims 1 and 3, the applicant's convention compares source and destination addresses and individual addresses in the permitted MAC address list. A typographical error is also corrected at claim 3 and new claim 5 includes additional specificity with respect to multicast and/or broadcast packets.

The invention relates to a security feature in network devices such as switches wherein security is applied in respect of individual media access control addresses. The device has a control which includes a memory for storing individual media access control addresses. This is the memory (table) 55 in Figure 5. This memory is selectively populated (for example by a network administrator).

The forwarding policy for a unicast packet is to compare both the source address and the destination address with the permitted addresses in the table. Thus provided that either the individual sender or the intended individual recipient is 'authorized', i.e., has a MAC address in the table, the forwarding of the packet is permitted. The point of this is that the system is immune to discovery processes that operate at the network layer (the usual case). MAC addresses are specific to individual devices and the unauthorized user (who will not have its source address in the permitted address table) has no means (via the network) of discovering an individual MAC address even if he/she knows the network address. That is, the incoming packet to the switch will not have the individual MAC address of the intended recipient. For multicast or broadcast packets special rules need to apply because the destination address in both cases is not an individual address.

Notwithstanding the Examiner's remarks, Doherty et al. do not operate in this way. Although the Examiner correctly asserts that Doherty provides lookups for the source and destination addresses individually, Doherty does so for a different purpose.

As described by Doherty in column 13 (the passage on which the Examiner relies) a packet is subject to three lookups, (1) for the source address in the database memory, (2) for the destination address in the database memory and (3) for the source/destination pair in the memory. The third is obviously not relevant to the present invention because the absence of the source/destination pair does not indicate whether either of the two addresses is in the memory. Moreover, if the SA/DA pair is not in the memory there is no 'prevention of forwarding'; the switch has to have recourse to a network protocol to discover the pair. It is true that if the source/destination pair is not in the table and, on being referred to an associated server, is deemed to indicate an impermissible connection (see Doherty column 5, lines 10-16); however, this (as the Examiner already seems to appreciate) is distinct from a test that discards the packet when neither address is found individually in the database and the discard action is not determined by the switch that receives the packet.

The lookup for the source address and destination address are not for the purpose of determining whether to discard the packet; they are employed to discover the node identification numbers of the source address node and the destination address node; these numbers are used for routing the packet (Doherty column 13, lines 16-20).

Doherty also provides a data structure in which source and destination addresses in the database memory are annotated. This is described in Doherty column 13, lines 33 to column 14, line 24 and importantly qualifies the purpose of the 'individual' lookups.

The data structure comprises, in essence, annotations for each entry in the forwarding database. Field 86 merely refers to the copying of the packet in addition to its normal forwarding. Field 88, if reset to 0, indicates that the destination address is 'unrestricted' and that a packet having this destination address is not subject to the source/destination pair lookup and processing. Likewise, field 92, if reset to 0, indicates that the source address is 'unrestricted' and that a packet having this source address is not subject to the source/destination pair lookup and processing. The Examiner may well regard the annotation fields as equivalent to permitted individual addresses. However, the interpretation is different; the absence of the annotation does not render the address a non-permitted address. In other words, if field 88 and field 92 are set to 1, the packet is not discarded; it is merely subject to the third lookup for the source address/destination address pair.

Accordingly, Doherty fails to anticipate because although it provides for individual lookups (in addition to his SA/DA pair lookup) it does not have a list of 'permitted' addresses and it does not prevent the forwarding of a packet when 'neither' address is in such a list. Doherty in effect says if the source or destination address is annotated as 'unrestricted' then the packet will be unconditionally forwarded; the inventors say if neither the source address nor the destination address is in the permitted list the packet is discarded.

More particularly, in relation to both claim 1 and claim 3, Doherty does not provide any equivalent of 'controllable storage of permitted individual media access control addresses; nor does it provide any means for restricting which prevents the forwarding of a unicast packet having a source address and a destination address when neither of those addresses in the unicast packet corresponds to a permitted media access control address.

In relation to claim 3, it should be noted that the data structure which annotates the MAC addresses in Doherty is the ordinary forwarding database (memory 54). Applicant's memory is distinct from the forwarding database.

Concerning claims 2 and 4, the Examiner has failed to take into account the features specified in the claims. Doherty provides (as is normal for any switch) an 'outmask' which is a bit mask that has a bit for each port on the switch and in accordance with the lookup processes (described in Doherty column 7, lines 14-35) is modified so that it has a bit set for each port from which a packet is to be forwarded. The Examiner has failed to identify, and Doherty fails to disclose the additional feature that this bit mask, which in the words of the claims is the 'port mask that identifies a port to which a packet may be forwarded according to media access control data in the packet' has to be further qualified so that the port mask identifies a port which is both a port to which a packet may be forwarded according to the media access control data in the packet (i.e., the result of the Doherty lookup) and a port in said list. Applicants employ in practice two bit masks which have to be ANDed together (see page 115, line 8) to produce the final bit mask for a multicast or broadcast packet; Doherty has no equivalent.

As earlier mentioned, new claim 5 includes limitations even beyond those of claim 4.

New method claims 6-10 are analogous to apparatus claims 1-5 respectively.

Accordingly, this entire application is now believed to be in allowable condition and a formal Notice to that effect is respectfully solicited.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: Larry S. Nixon
Larry S. Nixon
Reg. No. 25,640

LSN:vc
1100 North Glebe Road, 8th Floor
Arlington, VA 22201-4714
Telephone: (703) 816-4000
Facsimile: (703) 816-4100